(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2003 (13.11.2003)

PCT

(10) International Publication Number
WO 03/094418 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/AU03/00505

(22) International Filing Date: 30 April 2003 (30.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PS 2044 30 April 2002 (30.04.2002) AU

(71) Applicant (*for all designated States except US*): **INTEL-LIGUARD I.T. PTY LTD A.C.N. 098 700 344** [AU/AU]; 5 Binnie Street, EAST BRIGHTON, Victoria 3187 (AU).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): **KOWALSKI, Jacek, Piotr**, [PL/AU]; 34 Monkhouse Drive, ENDEAVOUR HILLS, Victoria 3802 (AU). **BAKER, Kenneth, George** [AU/AU]; 5 Binnie Street, EAST BRIGHTON, Victoria 3187 (AU).

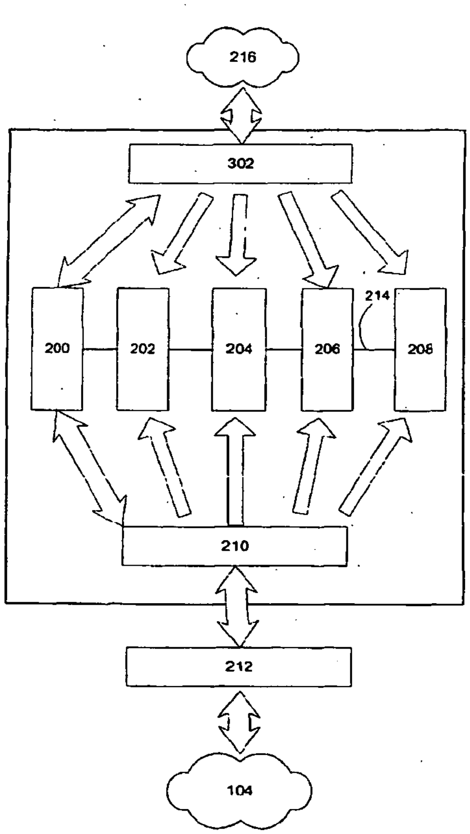
(74) Agents: **WEBBER, David, Brian** et al.; Davis Collison Cave, 1 Little Collins Street, MELBOURNE, Victoria 3000 (AU).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: A PACKET FILTERING SYSTEM



(57) **Abstract:** A packet filtering system for use with a communications network, including a filtering module (200) for filtering packets from the network (104, 216), and one or more analysis modules (202-208) operating in parallel and adapted to analyse packets from the network (104, 206) to determine whether to filter one or more of the packets and to communicate that decision to the filtering module (200). The system can include a device (210) for sending a copy of each packet to each of the analysis modules (202-208). The system can also include a second device (302) for sending a copy of each packet to each of the analysis modules (202-208). The modules (200-208) communicate with each other over a private communication medium (214) using a module control protocol.

WO 03/094418 A1

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A PACKET FILTERING SYSTEM

FIELD OF THE INVENTION

The present invention relates to a packet filtering system and a firewall system for use in a communications network.

BACKGROUND

The processing of data packets is an important feature of modern communications networks. In the case of the Internet, a packet in the network (*i.e.*, between the packet's source and destination) can be processed in a variety of ways, including filtering or dropping the packet if it satisfies certain criteria. For example, network security has become a primary concern for managers of computer systems and networks connected to insecure public communications networks such as the Internet. To reduce their vulnerability to attack, private networks and computer systems can be protected to some extent by using a hardware device or software module known as a firewall to filter data packets arriving from the insecure network. For example, as shown in Figure 1, a firewall system 100 is typically connected between an insecure communications network 104 and a computer system or private network 102. Data packets arriving from remote computer systems 106, 108 via the insecure network 104 are inspected by the firewall 100 to determine whether they are to be forwarded to the computer system or private network 102 or simply discarded, a process known as packet filtering. To provide the highest level of security, the firewall 100 can be programmed to block all incoming traffic apart from a small subset of allowed packets. For example, the firewall 100 may forward packets from the network 104 to the computer system or private network 102 provided that they originate from a particular source address, and that they are directed to a port that provides an allowed service. Any packets not meeting these criteria are discarded.

In cases where the firewall 100 is protecting a private network of computer systems rather than a single host, the firewall 100 may need to process an enormous amount of traffic, and this can constitute a bottleneck that limits the throughput of packets between the private network 102 and the public network 104. This is especially the case when the firewall is using complex traffic inspection and filtering rules that may include application layer information. It is therefore important to minimise the latency of the filtering process. Moreover, it is advantageous if the firewall 100 also monitors packets from the public network 104 to detect security attacks. However, this may require a substantial degree of data processing, and this will increase the latency of the firewall 100 and degrade throughput.

It is desired, therefore, to provide a packet filtering system and a firewall system that alleviate one or more of the above difficulties, or at least provides a useful alternative to existing packet filtering systems.

SUMMARY OF THE INVENTION

In accordance with the present invention, there is provided a firewall system for use with a communications network, said firewall system including a firewall module for filtering data packets from said network, and one or more analysis modules operating in parallel and adapted to analyse data packets from said network to detect security attacks and to communicate a detected security attack to said firewall module.

The firewall systems of the preferred embodiments use distributed processing by independent processing modules communicating via a communications protocol that controls the packet flow through the firewall module according to the results of traffic inspection and analysis processes executed in parallel by the analysis modules. Unlike prior art load balanced firewalls that distribute traffic between identical firewall modules on the basis of traffic flows, the firewall systems of the preferred embodiments use packet level parallelism to simultaneously process the same packet by a number of analysis

modules executing respective traffic inspection processes. This allows more advanced traffic processing than prior art firewall platforms without increasing network latency.

The present invention also provides a packet filtering system for use with a communications network, said packet filtering system including a filtering module for filtering packets from said network, and one or more analysis modules operating in parallel and adapted to analyse packets from said network to determine whether to filter one or more of said packets and to communicate a decision to filter one or more of said packets to said filtering module.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a communications network including a firewall and a number of hosts;

Figure 2 is a block diagram of a first preferred embodiment of a firewall system; and

Figure 3 is a block diagram of a second preferred embodiment of a firewall system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A firewall system, as shown in Figure 2, receives data packets originating from an insecure communications network 104, such as the Internet, monitors the packets for security attacks, and determines which packets to forward to a secure network 216 in order to protect the secure network 216. The firewall system includes several processing modules 200 to 208, and a flooding device 210. The flooding device 210 sends a copy of each packet received from the insecure network 104 to each of the processing modules 200 to 208. The processing modules 200 to 208 communicate over a private communication medium 214 that is independent of network traffic between the secure network 216 and the Internet 104. In the described embodiment, the flooding device 210 is a standard Ethernet

packet switch, such as a Cisco Catalyst 2900 XL, a Hewlett-Packard Procurve 4108GL, or a 3Com SuperStack 3 switch, and the processing modules 200 to 208 are single-board computers with a common backplane, such as ProLiant BL blade servers, available from Compaq. Each blade server includes a built-in Ethernet network interface connector (NIC), and these are used to simultaneously receive data packets from the flooding device 210. The backplane provides the private communication medium 214, hereinafter referred to as the backplane 214, that allows the processing modules 200 to 208 to communicate with each other, independently of network traffic.

The firewall system receives data packets from a layer 3 routing device 212, which is preferably a secure sockets layer (SSL) accelerator providing high speed hardware-based encryption and decryption of SSL data packets. The SSL accelerator 212 is a standard SSL accelerator such as a SonicWALL SSL-R6 Accelerator from SonicWALL, Inc., an Intel® NetStructure™ 7185 e-Commerce Director, or a NetSwift 2012 appliance from Rainbow Technologies. However, if SSL support is not required, the layer 3 routing device 212 can alternatively be a standard router.

The processing modules 200 to 208 include a filtering or packet gateway module (PGM) 200, and analysis modules 202 to 208. The PGM 200 is a layer 3 and 4 filtering firewall module that performs standard packet filtering functions. The monitoring of traffic to detect security attacks targeted at applications is performed by the analysis modules 202 to 208. The analysis modules 202 to 208 include a Denial of Service Attack Detection Module (DOSADM) 202, and Inspection Specific Modules (ISMs) 204 to 208. The DOSADM 202 analyses overall traffic patterns to detect denial of service attack indicators, including port scanning and SYN flooding, and performs temporal analysis of traffic flow patterns. The ISMs 204 to 208 execute application layer (or layer 5, 6, and 7) inspection and analysis processes, including data mining processes for detecting network traffic anomalies. Data mining processes are advantageous because they are capable of detecting unknown security attacks, as described in W. Lee and S.J. Stolfo, *Data Mining Approaches for Intrusion Detection*, Proceedings of the 7th USENIX Security Symposium, 1998. The

DOSADM 202 analyses temporal traffic flow patterns in order to detect denial of service attacks such as port scanning and SYN flooding.

A data packet arriving at the SSL accelerator 212 from the Internet 104 is inspected by the SSL accelerator 212. If the data packet is an SSL packet including encrypted contents, the SSL accelerator 212 decrypts the packet contents and forwards the decrypted packet to the flooding device 210 of the firewall system. Otherwise, if the data packet is not an SSL packet, it is forwarded to the flooding device 210 without modification. The flooding device 210 receives the packet and sends a copy of it to each of the processing modules 200 to 208. Because the flooding device 210 is a standard Ethernet packet switch, packet flooding is achieved by altering the address resolution protocol (ARP) in the PGM 200 so that it always responds to ARP requests from the SSL accelerator 212 with a non-existent medium access control (MAC) layer address. This MAC address is then used by the SSL accelerator 212 in front of the processing modules 200 to 208 to send layer 2 frames. Because the MAC address used does not exist in this network segment, when a frame with this non-existent MAC address is forwarded by the switch 210, it floods traffic to all its ports, therefore sending a copy of the same frame to all processing modules 200 to 208. In an alternative embodiment, the flooding device 210 is an Ethernet packet switch that executes a modified firmware process that floods packets into selected ports irrespective of entries in its switching table.

The PGM 200 is the gateway for filtering traffic between the Internet 104 and the secure network 216. The PGM 200 performs standard layer 3 and 4 packet filtering (administrative or dynamic), maintaining state information about every connection/traffic flow and allowing dynamic access control for return traffic from the secure network 216 to the Internet 104. The state information includes source and destination IP addresses, protocol number, and source and destination ports, where appropriate. The mechanism for maintaining state information is based on a flow hash table, a flow hashing function, and a binary tree structure. The flow hashing function is preferably a weighted sum modulo N of all the octets of the source IP address with the weights being selected mutually prime numbers. However, it will be apparent that alternative flow hashing functions can be used.

Because the values of the hash function are not unique for every source address, the hash values are used to index an array of size *N* that stores pointers to the roots of binary trees that allow rapid retrieval of the state information for a particular traffic flow. Given a source IP address, a hash value is determined and used to locate the binary tree for those source addresses that give rise to that hash value. The state information for that particular source address is then located by navigating branches of the binary tree based on the address value.

The network interfaces of the analysis modules 202 to 208 are set to promiscuous mode to receive all incoming packets. However, any packets blocked by the PGM 200 at layer 3 or 4 can also be discarded by each analysis module to avoid unnecessary processing of packets that are already blocked. Alternatively, one or more of the analysis modules 202 to 208 can accept and analyse packets blocked by the PGM 200 to detect a security attack. For example, a packet sent from an unblocked address but addressed to a blocked destination port number may be part of a network scan, and if this attack is detected by an analysis module, then that analysis module can instruct the PGM 200 and the other analysis modules to block all packets sent from that address. In any case, each analysis module is programmed to only accept and process packets matching that module's requirements. Each of the analysis modules 202 to 208 is configured to accept either TCP packets only or UDP and other non-TCP packets only. Analysis modules accepting TCP packets use the same flow hashing function as that used by the PGM 200; however, other than discarding packets blocked at layer 3, the only additional layer 3–4 filtering that they perform is to check the status of the SYN flag. If the SYN flag of a packet is off, this indicates that the corresponding TCP connection was accepted during the TCP connection setup phase and was not administratively blocked by the PGM 200. Consequently, packets with the SYN flag off may be processed, whereas packets with the SYN flag on are discarded. In contrast the DOSADM module 202 accepts all packets for analysis, including those with the SYN flag on, in order to detect denial of service attacks. An analysis module 202 to 208 detecting a security attack notifies the PGM 200 and the other analysis modules to reject packets originating from the attacking IP address. This can be achieved by

spoofing TCP reset packets if the packets are TCP packets, and otherwise by discarding the packets.

The processing modules 200 to 208 communicate amongst each other using a Firewall Module Control Protocol (FMCP) on the backplane 214. FMCP is implemented as an application layer protocol transported by UDP. However, it will be apparent that it can alternatively be implemented as a transport protocol with its own protocol number. If an FMCP message is intended for all modules, then it is broadcast to the backplane 216. FMCP is used for sending service rate reduction messages and module configuration messages, as described below. In particular, FMCP is used to send security alerts from an analysis module that detects a security attack to the other processing modules. FMCP security alert messages include the hash value and IP address of the offending source IP address. Because the processing modules 200 to 208 use the same flow hashing algorithm, sending the hash value along with the corresponding IP address eliminates the need for the receiving module to calculate the hash again, thereby speeding up the processing of the message. The PGM 200 receives the security alert message and then prevents the security attack on the secure network 216 by blocking the IP address of the originator of the attack or by resetting the offending TCP connection. Packets originating from a blocked IP address are discarded by the PGM 200. The analysis modules 202 to 208 also receive the FMCP security alert and subsequently discard packets from the blocked address to avoid unnecessary processing.

Unlike a load-balanced firewall, the firewall system uses more than one processor to process a single packet in parallel, decreasing latency. A load-balanced firewall distributes traffic to different processors on a per flow basis (a flow being defined as a collection of packets received within a specific timeout interval from the same source IP address/protocol port number and destined to the same IP address/ port number). Each processor applies filtering and analysis algorithms on packets belonging to the same flow in a sequential manner *eg.*, *A1*, *A2*, ..., *An*, and therefore the processing time for a packet is *T1* + *T2* + ... + *Tn*. In contrast, the firewall systems described herein execute several analysis processes on respective analysis modules 202 to 208 for the same packet, and the

processing time for the packet is therefore given by max(*T1*, *T2*, ..., *Tn*). In situations where the different analysis processes result in very different computational loads, the analysis modules 202 to 208 can perform flow-based load balancing to reduce the overall processing time. For example, if an analysis process *A2* requires twice as much processing time as an analysis process *A1*, and the analysis process *A1* is executed by a single ISM, two other ISMs can execute analysis process *A2* in parallel, each ISM processing a complementary subset of received packets determined by a flow based hash function. In general, if the queuing service rates for analysis processes *A1* and *A2* are respectively *R1* and *R2* and $R1=k*R2$, the number of ISMs executing analysis process *A2* can be up to the nearest integer upper bound of k. This technique increases the throughput of the firewall system and reduces the queuing delay for slower analysis processes.

As an alternative to the service rate equalization described above, a method based on the packet queue length of the slowest process can be used, as follows. If the length of the queue of packets waiting to be processed by the slowest process exceeds a threshold length, an FMCP message is sent by the ISM executing the slowest analysis process to the ISMs executing the faster analysis processes, instructing the latter to slow their service rates to the service rate of the slowest process in order to avoid overrunning the packet buffer of the ISM executing the slowest process.

In a second preferred embodiment, the firewall system also includes a further, second flooding device 302 identical to the first flooding device 210, but located between the private network 216 and the processing modules 200 to 208, as shown in Figure 3. The second flooding device 302 sends a copy of each packet received from the private network 216 to each of the processing modules 200 to 208 in order to analyse network traffic originating from the private network 216. This allows additional traffic analysis to be performed, and is particularly useful when the firewall system is used between two private networks, in which case the firewall system protects each private network from attack from the other private network.

Although the firewall systems described above include four analysis modules 202 to 208, it will be apparent that any number of analysis modules can be included, providing there is at least one to analyze traffic independently of the PGM 200.

Although the firewall systems described above are based on blade server technology, it will apparent that the firewall system can alternatively be implemented on a single card having multiple processors, or even on a single integrated circuit having multiple processors. Furthermore, it will be apparent that alternative architectures can be used if other technologies are used. For example, rather than have each of the analysis modules 202 to 208 independently inspect every received packet in order to determine whether it is to be rejected prior to performing any module-specific analysis, this inspection could instead be performed only by the PGM 200 if the flooding device 210 and the analysis modules 202 to 208 are located behind the PGM 200.

It will be apparent that although the firewall system is described above as filtering packets between an insecure and a secure network, the firewall system can be used to filter packets between any combination of hosts and/or networks, whether notionally secure or insecure.

Moreover, by omitting the DOSADM module 202, a general-purpose packet filtering system is provided that is not necessarily concerned with network security at all, and can be used to filter received packets based on arbitrary criteria. For example, the system may filter packets at least potentially containing sexually explicit or otherwise undesirable content. In this embodiment, one or more analysis modules, such as the analysis modules 202 to 208 (which may or may not include a data mining module), can be used to perform any desired analysis of received packets to determine whether any of these packets should be filtered, and to communicate any decision to filter packets to the PGM 200.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.

CLAIMS:

1. A firewall system for use with a communications network, said firewall system including a firewall module for filtering data packets from said network, and one or more analysis modules operating in parallel and adapted to analyse data packets from said network to detect security attacks and to communicate a detected security attack to said firewall module.

2. A firewall system as claimed in claim 1, including a device for sending each of said data packets to each of said one or more analysis modules.

3. A firewall system as claimed in claim 2, wherein said device also sends each of said data packets to said firewall module.

4. A firewall system as claimed in claim 1, wherein said one or more analysis modules includes a module adapted to detect a denial of service attack.

5. A firewall system as claimed in claim 1, wherein said one or more analysis modules includes at least one module for performing data mining on said data packets to detect a security attack.

6. A firewall system as claimed in claim 1, including a private medium for communication between said firewall module and said one or more analysis modules.

7. A firewall system as claimed in claim 6, wherein said communication is based on a firewall module control protocol for communication of security information between said firewall module and said one or more analysis modules.

8. A firewall system as claimed in claim 1, wherein a detected security attack is communicated to said one or more analysis modules.

9. A firewall system as claimed in claim 8, wherein communication of a detected security attack includes a network address associated with said security attack and a corresponding hash value.

10. A firewall system as claimed in claim 1, including a secure services layer (SSL) accelerator for decrypting encrypted packets received from said network.

11. A firewall system as claimed in claim 2, including a second device for sending each data packet destined for said network to each of said one or more analysis modules.

12. A firewall system as claimed in claim 3, wherein each of said one or more analysis modules filters data packets received from said device.

13. A firewall system as claimed in claim 1, including a device for receiving filtered data packets from said firewall module and for sending each of the received data packets to each of said one or more analysis modules.

14. A packet filtering system for use with a communications network, said packet filtering system including a filtering module for filtering packets from said network, and one or more analysis modules operating in parallel and adapted to analyse packets from said network to determine whether to filter one or more of said packets and to communicate a decision to filter one or more of said packets to said filtering module.

15. A packet filtering system as claimed in claim 14, including a device for sending each of said packets to each of said one or more analysis modules.

16. A packet filtering system as claimed in claim 15, wherein said device also sends each of said packets to said filtering module.

17. A packet filtering system as claimed in claim 16, wherein each of said one or more analysis modules filters packets received from said device.

18. A packet filtering system as claimed in claim 14, including a device for receiving filtered packets from said filtering module and for sending each of the received packets to each of said one or more analysis modules.

19. A packet filtering system as claimed in claim 14, wherein said one or more analysis modules includes at least one module for performing data mining on said packets to determine whether to filter one or more of said packets.

20. A packet filtering system as claimed in claim 14, including a private medium for communication between said filtering module and said one or more analysis modules.

21. A packet filtering system as claimed in claim 20, wherein said communication is based on a module control protocol for communication of packet-related information between said filtering module and said one or more analysis modules.

22. A packet filtering system as claimed in claim 14, wherein a decision to filter one or more of said packets is communicated to said one or more analysis modules.

23. A packet filtering system as claimed in claim 15, including a second device for sending each packet destined for said network to each of said one or more analysis modules.

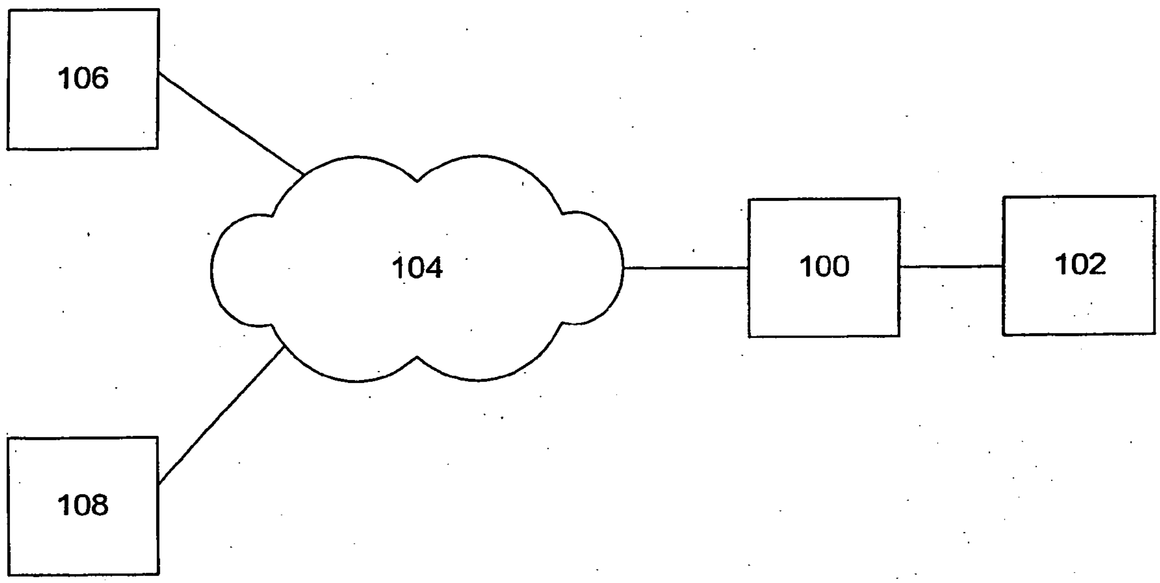


Figure 1

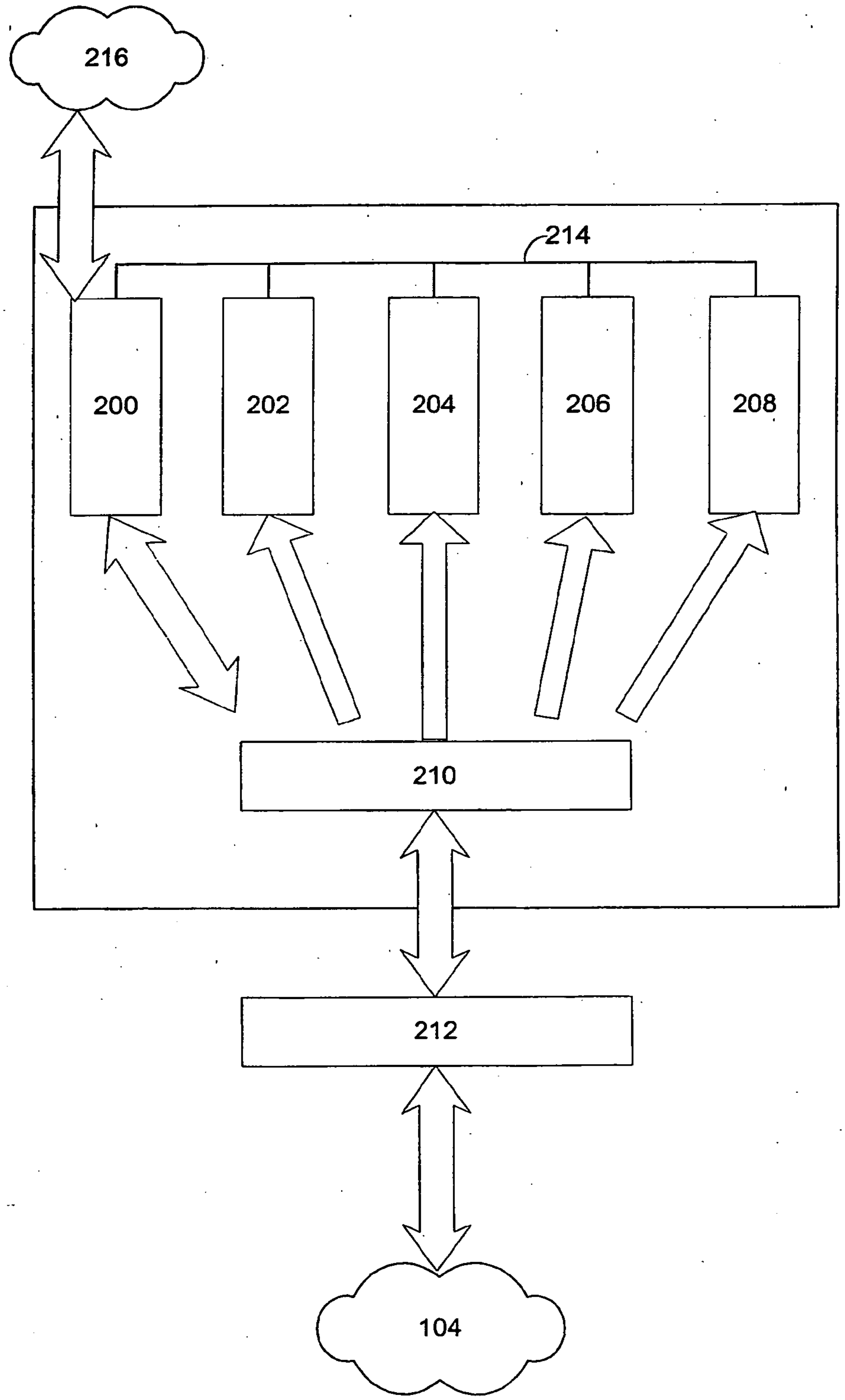


Figure 2

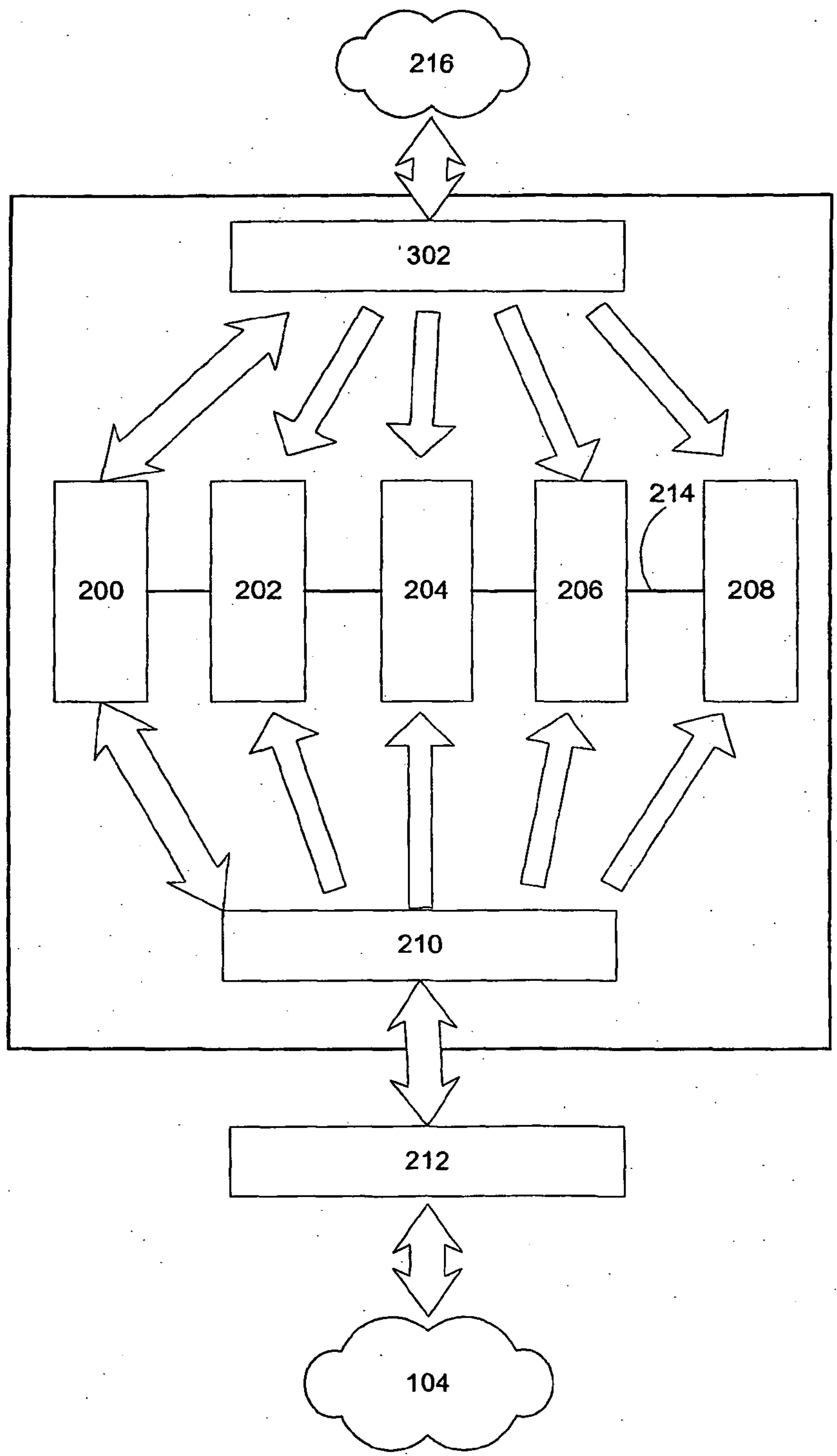


Figure 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU03/00505

A.	**CLASSIFICATION OF SUBJECT MATTER**
Int. Cl. ^{7}:	H04L 9/00
According to International Patent Classification (IPC) or to both national classification and IPC	
B.	**FIELDS SEARCHED**
Minimum documentation searched (classification system followed by classification symbols)	
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched	
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT, USPTO: FIREWALL, PACKET, NETWORK, ANALYSE AND SIMILAR TERMS	

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	WO 02/099644 A1 (PSYNAPSE TECHNOLOGIES, LLC) 12 December 2002 whole document	1-23
X	WO 01/80480 A1 (JOYCE, JAMES B.) 25 October 2001 whole document	1-23
A	US 6219706 B1 (FAN et al.) 17 April 2001 whole document	1-23

☐ Further documents are listed in the continuation of Box C   ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 18 June 2003	Date of mailing of the international search report 26 JUN 2003
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **SUSHIL AGGARWAL** Telephone No : (02) 6283 2192

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU03/00505

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	02/099644	US	2002188864				
WO	01/80480	AU	47735/01	EP	1279248	US	6519703
US	6219706	NONE					

END OF ANNEX

BEST AVAILABLE COPY